KPDP for CSS

# KPDP for CSS:

## DVD Content Scramble System

## Key Protection Data for CSS Generation Program

## User's Guide Version1.1

*for CSS Spectification Version 0.90 & 0.96*
*October, 1, 1999*

# Secured Disc Key Data/Encrypted Title Keys

1. Client requests Secured Disc Key Data/Encrypted Title Keys.
2. DVD CCA sends to client the CSS Key Input Program & Guide Book for Content Providers, Authoring Studio, DVD Disc Replicator.
3. Client creates Input for Disc Key/Title Keys by using the CSS Key Input Program on their PC.
4. Client makes Key Input floppy disc.
5. Client sends floppy disc to DVD CCA.
6. DVD CCA makes "Secured Disc Keys/Encrypted Title Keys" using Sun Work Station.
7. After process is complete, DVD CCA sends client back their floppy disc containing Secured Disc Keys/Encrypted Title Keys.

199// 7// 9
(Ver3.2a)

# Request Sheet to issue the Encrypted Keys


Name of Company : DVD Copy Control Association

Name of Contact Person : Paula Williams

Address of Contact Person : 225 B Cochrane Circle Morgan Hill CA 95037 USA

Phone Number of Contact Person : (408) 776-2014

FAX Number of Contact Person : (408) 779-9291


Applicant Number : 1

| Disk Key | 111111111111 | |
|---|---|---|
| | CGMS | Title Key Number |
| Title Key(1) | 11 | 122222222222 |
| Title Key(2) | 11 | 123554 |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

## 1.Overview

KPDP for CSS is a program which generate Key Protection Data for CSS. In this paper, we describe the basic operation of KPDP for CSS (which based on CSS Specification Version 0.90 and 0.96).

Key Protection Data for CSS is

(i) Secured Disc Key Data
(ii) Encrypted Title Key
(iii) Authentication Control Code

and so on(see detail in Content Side Guide Book)..

The issue of the Key Protection Data of CSS takes three steps shown below,

1. The Content Side generate the "Request Floopy Disc for CSS" and send it to DVD CCA.
2. DVD CCA generate "Key Protection Data for CSS" and stored new files to the "Requesting Floopy Disc for CSS".
3. DVD CCA send back the new "Requesting Floopy Disc for CSS" to the Content Side.

KPDP for CSS is softwares to generate the "Key Protection Data for CSS" from the Request Data in the "Requesting Floopy Disc" .

KPDP for CSS include these three programs,

(a) v_check.sh:
detect which version of specification the "Requesting Foppy Disc" based on. It is a shell script on UNIX WS.

(b)sma31:
Key Protection Data generation Program based on the Version 0.90 of CSS specification.

(c)css:
Key Protection Data generation Program based on the Version 0.96 of CSS specification.

## 2.Basic Operation

### (1) Login to the Work Station

First, login to the Work Station which KPDP for CSS is installed as the KPDP for CSS operator.

login:_____
passwd:_____

### (2) Open the "command tools"

When you login to the Work Station as KPDP for CSS operator, the Openwindow has been starting. Second, you start up "command tool".

(2.1)Point the cursor on the back ground(wallpaper) and the click the right bottom of the mouse.

(2.2)Select the "Programs" on "Workspace" and select the "command tools" on "Programs". Then "command tool" window is opened.

You point the cursor on the "command tool" and the click the left bottom of the mouse. Steps from (3) to (7) are done on the "command tools" window.

### (3) Go to the KPDP for CSS installation directory

And you go to the directory which KPDP for CSS is installed.

css@ultra% **cd video/prog*(return)***

*In the case of the practice, you go to the practice directory instead of the directory "video/prog".*
*css@ultra%* ***cd practice(return)***

## (4) Insert the "Request Floppy Disc for CSS"

Insert the "Request Floppy Disc" sent from the Content Sider.

## (5) Version Check

Next, you run the "v_check.sh" program to check the version of the CSS specification which the "Requesting Floppy Disc" is based on.

css@ultra% v_check.sh*(return)*

V_check.sum
↑ underscore

Then "v_check.sh" program begin to run, and show the version of the CSS specification which the "Request Floppy Disc" based and program name which you have to run(shown in Fig<2.1>)

```
*** v_check detect the "Requesting Floppy Disc" ...
*** CSS Ver.0.90 file found.
(OK) please use "sma31" program.
```

(a)in the case of "CSS Version 0.90"

```
*** v_check detect the "Requesting Floppy Disc" ...
*** CSS Ver.0.96 file found.
(OK) please use "css" program.
```

(b)in the case of "CSS Version 0.96"

```
*** v_check detect the "Requesting Floppy Disc" ...
.....
        (ERROR) please check the FD.
```

(c)in the case of illegal data format error

```
*** v_check detect the "Requesting Floppy Disc" ...
(Error) *** FD file List can't be read(1).
```

(d)in the case of "v_check" error

**Fig<2.1> Output of the v_check.sh**

Output of "v_check.sh" is

(i) as same as Fig<2.1>(a), the "Requesting Floppy Disc" is base on CSS specification Version 0.90 and you must run the program "sma31" (go to step(6)(a)).

(ii) as same as Fig<2.1>(b), the "Requesting Floppy Disc" is based on CSS specification Version 0.96 and you must run the program "css" (go to step(6)(b)).

(iii) as same as Fig<2.1>(c), the file format of "Requesting Floppy Disc" is illegal. Please check that you insert the correct FD or not, and contact to the programmer.

(iv )as same as Fig<2.1>(d), v_check program error occured. Then you don't do anything on the WS and contact to the programmer.

(*) during the "v_check.sh" operation, "File Manager" window is opened, but please ignore this window.

## (6) Run the KPDP for CSS

(a)Run "sma31"(CSS Version 0.90)

When the "Requesting Floppy Disc" is based on the CSS Version 0.90, you have to run "sma31". The “sma31” program need the “Client Name” as the command line option. "Client Name" is the name to identify the requesting appplicant(= Content Side) and is specified by the DVD CCA. "Client Name" must be within 10 characters which consists of alphabet(‘a’～’z’, ‘A’～’Z’) or digits(‘0’～’9’). For example, in the case of the requesting applicant is "American Beauty Company", you specify "ABC" as a Client Name.

```
css@ultra% sma31 ABC(return)
```

In the beginning, "sma31" ask you than specified Client Name is correct or not.

When the Client Name is correct, you input 'Y'. Otherwise, you input 'N' and restart the program with the correct Client Name.
When the KPDP for CSS begin to run, some messages are displayed. In case of the success of "sma31", such a messages shown in Fig<2.2>("----- END ----------" shows the success of "sma31").

```
rm: INPUT.TXT: No such file or directory
Copying INPUT.TXT
----- wait ! -------in check_data_dir():directory:[./Data] is not found.
in check_data_dir():making dir:[./Data].
I Get Dir Name:[./Data/00005001]
Copying SMA3_FD.TXT
Copying SMA3_DK.TXT
Copying SMA3_ED.BIN
Copying SMA3_TN.TXT
Copying SMA3_TK.TXT
Copying SMA3_ET.BIN
Copying SMA3_AC.BIN
Removing INPUT.TXT
----- END ----------
```

**<Fig.2.2> success messages of "sma31"**

If error has happened, some error messages are displayed. So you must write down the error messages and contact to the programmer.

(b)Run "css"(CSS Version 0.96)
When the "Requesting Floppy Disc" is based on the CSS Version 0.96, you have to run "css".

css@ultra% ***css(return)***

When the KPDP for CSS begin to run, some messages are displayed. In case of the success of "css", such a messages shown in Fig<2.3>("(CSS-0.96):CSS Key Protection Data Generation Success." shows the success of "css").

```
rm: CSS-V-input.txt: No such file or directory
Copying CSS-V-input.txt
*****************************************************
* (CSS-0.96):DVD Content Scramble System
* (CSS-0.96):Key Protection Data Generation Program
* (CSS-0.96):[css-kpdp-99-09-16-01]
*****************************************************

(CSS-0.96):Input Data Check...OK

in check_data_dir():directory:[./Data] is not found.
in check_data_dir():making dir:[./Data].
(CSS-0.96):Data Request is acceped...

(CSS-0.96):Setting Disk Key...OK
(CSS-0.96):Setting Title Key...OK
(CSS-0.96):Setting TK0(VM Title Key)...OK
(CSS-0.96):Setting TK100(JP Title Key)...OK
(CSS-0.96):Tk Encryption(Key:Dk)...OK
(CSS-0.96):TK0(VM Tk) Encryption(Key:Dk)...OK
(CSS-0.96):TK100(JP Tk) Encryption(Key:Dk)...OK
(CSS-0.96):Dk Encryption(Key:Dk)...OK
(CSS-0.96):Dk Encryption(Key:Mk)...OK
(CSS-0.96):Dk Test...OK
(CSS-0.96):make data directory success.
(CSS-0.96):Open Key Protection Data Files.....OK
(CSS-0.96):Key Protection Data Generating Successfully Done.....
(CSS-0.96):css_start() success.
(CSS-0.96):data stored directory is [./Data/00005001]
Copying CSS-V-contact.txt
Copying CSS-V-FD.TXT
Copying CSS-V-DK.TXT
Copying CSS-SDKD.BIN
```

```
Copying CSS-V-TK0.TXT
Copying CSS-V-ETK0.BIN
Copying CSS-V-TN.TXT
Copying CSS-V-TK.TXT
Copying CSS-V-ETK.BIN
Copying CSS-V-TK100.TXT
Copying CSS-V-ETK100.BIN
Copying CSS-V-AC.BIN
Removing CSS-V-input.txt
(CSS-0.96):CSS Key Protection Data Generation Success.
```

**<Fig.2.3> success messages of the "css"**

If error has happened, some error messages are displayed. So you must write down the error messages and contact to the programmer.

## (7) Eject the "Request Floppy Disc"

When the KPDP for CSS has succeed, the Key Protection Data for CSS is stored into the "Request Floppy Disc". Then, you can eject the FD and send back to the requesting applicant.

```
css@ultra% eject(return)
```

(8) You ~~shall~~ must back to the Home directory.

```
css@ultra% cd (return)
```

## 3. Trouble Shooting

When KPDP for CSS finished with error messages, you must note the error messages and judge the kind of errors.

There are two kinds of errors which KPDP for CSS made.

1. Illegal Key errors:

   The errors based on the illegal Key Data specified by the requesting applicant.

2. Other errors

### 3.1 Illegal Key errors

In case the error happened with error messages shown in Fig.3.1, the Key specified by the requesting applicant is not suitable for CSS. Then DVD CCA should tell it to the requesting applicant and let the applicant request again with new Keys.

```
****************************************
*** ILLEGAL Title Key is set ***
***       title key[X]:[XX][XX][XX][XX][XX] ] is not suitable for CSS ***
*** Please Change title key ***
****************************************
```

(i) ILLEGAL Title Key

```
****************************************
*** ILLEGAL Disc Key is set ***
***       title key[X]:[XX][XX][XX][XX][XX] ] is not suitable for CSS ***
*** Please Change title key ***
****************************************
```

(ii) ILLEGAL Disc Key

**<Fig.3.1> illegal Key error messages**

### 3.2 Other errors

When the error happened with other error messages shown in the Fig.3.1, note the error messages and contact to the programmer of KPDP for CSS.

## 4. Management Information

In this section, we describe the way to manage the generated Key Protection Data for CSS.

### 4.1 Data management process

To management the generated Key Protection Data for CSS, we numbered each Key Protection Data.

The first Key Protection Data for CSS is numbered 1, and the second Key Protection Data for CSS is numbered 2, then the N-th Key Protection Data for CSS is numbered N.

During the Key Protection Data generating process, "sma31" or "css" program number newly generating Data X, and generate the directory X, then stored Key Protection Data into this directory. The current serial number is stored in ".serial" file.

By now, we generated 2705 Key Protection Data for CSS in CSS Interim Organization.

So, generated Data is stored in from directory 0001 to directory 2705 each other. And 2705 is stored in ".serial" file.

The serial number stored in the ".serial" file is very important data and YOU MUST NOT DELETE OR MODIFIED ".serial" FILE.

To maintain the uniqueness of serial number, Key Protection Data for CSS generated in CSS Interim Organization is numbered from 1 and limited to 5000, and Key Protection Data for CSS generated in DVD CCA is numberd from 00005001 and limited to 99999999. But we can extend the limit of serial number by modify program. So, please contact to the programer, if you need the extentention of the limit.

### 4.2 applicant DataID

The applicant DataID is the number specified by the requesting applicant(=Content Side) to manage the Key Protection Data by each applicant(client).The applicant DataID is written in the "Requesting Floppy Disc for CSS".

"Sma31" or "css" store DataID in the ".XXX_serial" file. In the case of "sma31", "XXX" is applicant(client) name which you specified as the command line option .

In the case of "css", XXXX is read from the "Requesting Floppy Disc".

The applicant DataID stored in the ".XXXX_serial" file is very important data and YOU MUST NOT DELETE OR MODIFIED ".XXXX_sedrial" FILE.

**4.3 log file**

Key Protection Data for CSS generating process is logged in "log" file stored in each data